оплати, що сприяють підвищенню привабливості впровадження даної технології банками.

Для поліпшення ідентифікації безпеки пропонується також використовувати метод автентифікації в роботі автомобільного іммобілайзера як RFID (Radio Frequency IDentification) – мітки, яка є невід'ємною частиною ключа сучасного автомобіля. Це мікросхема, яка містить пам'ять з секретним кодом, мініатюрний передавач і приймач радіосигналу. Енергії електромагнітних хвиль вистачає, щоб мікросхема відправила у відповідь секретний код. Отримавши правильну відповідь, іммобілайзер дозволяє блоку управління двигуном включитися. У найближчому майбутньому автомобільний ключ може взяти на себе куди більше функцій, ніж просте відкривання дверей і захист від викрадення. Еволюція буде пов'язана з поширенням технології передачі даних на короткі відстані NFC. Пристрої, сумісні з NFC, такі як автомобільний ключ, мобільні телефони, комп'ютери, банкомати, можуть обмінюватися даними, тільки перебуваючи на відстані щонайменше 10 см.

Список бібліографічних посилань

1. MasterCard Cloud-Based Payments Product Description, MasterCard Digital Enablemet Service, 2015.

2. Kulkarni M., Im D. J., Saputra S. J. SamsungPay Payment Method // Maheshkk.github.io. 15 September 2016. URL: https://maheshkk.github.io/webpayments/proposals/SamsungPay-payment-method.html [Accessed: 18 Jul 2018].

3. MasterCard Cloud-Based Payments Credential Managment System Functional Description, MasterCard Digital Enablemet Service, 2015.

Одержано 01.11.2018

УДК 621.34

Василь Миколайович КЛОЧКО,
студент 2 курсу факультету № 6
Харківського національного університету внутрішніх справ

ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖАХ РУХОМОГО ЗВ'ЯЗКУ

На сучасному етапі розвитку людство майже не уявляє свого існування без звичного мобільного зв'язку, тому питання дослідження та вдосконалення моделей захисту інформації в мережах рухомого зв'язку постає дедалі частіше. В основі забезпечення захисту інформації в мережах рухомого зв'язку лежать законодавчі та нормативно-правові норми, морально-етичні звичаї суспільства, організаційні та апаратно-програмні засоби та способи функціонального забезпечення інформаційної безпеки цифрових систем, каналів, мереж зв'язку.

Необхідно зауважити, що забезпечення надійного захисту інформації в мережах рухомого зв'язку перш за все, залежить від наявності певних чинників, які безпосередньо забезпечують та впливають на ступінь захищеності інформації в мережі, а саме:

– врахування особливостей відповідної технології зв'язку в процесі розробки необхідної моделі комплексного захисту інформації згідно способів та властивостей передавання/приймання фізичного сигналу, самого фізичного середовища – каналу, мережі, апаратно-програмних засобів цифрових систем зв'язку;

– наявність математичної моделі сигналу або каналу, в якій закладено параметри якісного і кількісного рівнів взаємозв'язку вхідного і вихідного сигналу.

Загальноприйнятими та найпоширенішими стандартами стільникового зв'язку в Європі є GSM (Global System for Mobile Communications), та UMTS (Universal Mobile Telecommunications System), наразі поряд з ними також функціонує стандарт стільникового зв'язку LTE. Враховуючи особливості кожного стандарту - необхідно використовувати притаманні лише йому технології, методи та засоби захисту інформації.

Найбільше розповсюдженими стандартами цифрового стільникового зв'язку наразі є GSM. Для визначеного стандарту у світі активно використовують такі технології захисту інформації, як: автентифікація повідомлень, верифікація, біометрія, шифрування/дешифрування (криптомодулі), зміна частот зі зміною місця, передавання пакетів на різних частотах, системи контролю доступу до базової станції, шумоподібний сигнал з кодовим доступом, канальне кодування/декодування, скремблювання.

Щодо методів захисту, необхідно зауважити, що багатьма країнами та операторами стільникового зв'язку активно використовується шифрування (RSA), яке в подальшому вимагає коди автентифікації абонента. Враховуючи, що ст. 31 Конституції України гарантує кожному таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції, на операторів зв'язку автоматично покладається обов'язок з забезпечення такої таємниці, через що було запроваджено методи секретності абонента, секретності передавання даних, секретності напрямів з'єднання абонентів, обмеження доступу до центрального вузла, управління роботою мережі та контроль цієї роботи, а також забезпечення конфіденційності на канальному та мережевому рівнях [1].

Науковцями пропонується впровадження нової методології з захисту інформації при використанні GSM зв'язку, наприклад,

започаткування стратегії ідентифікації користувача за допомогою перевірки правильності його реакції на непередбачуваний запит системи.

Засоби захисту інформації необхідно впроваджувати на усіх рівнях передачі сигналів. Технологія GSM зв'язку в своїй основі має чотири рівні: канальний, мережевий, транспортний та прикладний рівні.

Канальний та мережевий рівень схожі за своїми властивостями, тому для їх належного захисту доцільно використовувати однакові засоби захисту інформації, наприклад, в SIM-модулі передбачена наявність зберігання симетричного ключа, який відомий лише центру автентифікації вузла зв'язку. Визначений ключ застосовується при автентифікації абонента та для шифрування інформації перед передаванням.

Безпека на транспортному рівні забезпечується за допомогою посилених сертифікатів SSL та TLS, які є протоколами, що гарантують безпечне передавання даних у мережі, комбінуючи криптографічне шифрування у системі з відкритим ключем та блокове шифрування даних. Також на визначеному рівні використовується складний протокол управління сесією для встановлення, відновлення, закінчення зв'язку, автентифікація клієнта/сервера через сертифікат X.509 [2].

На прикладному рівні частіше за все використовують хешування для генерування MAC, а також універсальне шифрування: RC5; 3DES, чи цифровий підпис: PKI, RSA, ECDSA, ECC.

Серед універсальних систем стільникового зв'язку найпоширенішою на території країн СНГ є технологія UMTS (Universal Mobile Telecommunications System).

Для захисту інформації в мережі UMTS зазвичай використовується автентифікація повідомлень, верифікація, шифрування/дешифрування (криптомодулі), зміна частот із зміною місця, передавання пакетів на різних частотах, системи контролю доступу до базової станції та мережевого обладнання, шумоподібний сигнал з кодовим доступом, віртуальні приватні мережі.

Щодо методів захисту інформації доцільно використовувати наступні: перевірка справжності абонента за допомогою логіну/паролю користувача, проте така система не є надійною та може бути сфальсифікована за умови використання лише неї. Для унеможливлення несанкціонованого доступу до даних абонента передбачено використання методів забезпечення секретності абонента, технологій, які застосовуються для передавання даних, та напрямів з'єднання абонентів [3].

Засоби захисту інформації також застосовуються в залежності від рівня трансляції сигналу зв'язку.

На фізичному рівні доцільно використовувати: сигнальне скремблювання безпровідного зв'язку, а також можливості частотного скремблювання радіозв'язку, враховуючи, розширений спектр частот, коли кожний фрагмент ідентифікується цифровим кодом, який знають термінал отримувача та базова станція, при чому жодний інший термінал не може отримати передавання, так як, для кожного передавання існують мільйони кодових комбінацій.

Для забезпечення конфіденційності на канальному та мережевому рівнях активно застосовується шифрування кожного сегмента дейтаграми перед передаванням, ключ зазначено шифрування використовується в автентифікації та шифруванні кадрів TDMA перед передаванням.

Транспортний рівень забезпечує захищеність даних за допомогою посилених сертифікатів SSL та TLS – це протоколи, що гарантують безпечне передавання даних у мережі, комбінуючи криптографічну систему з відкритим ключем та блокове шифрування даних, а також відкритий ключ (RSA) для обміну ключами сесії (RC4 та інші) для групового шифрування.

На прикладному рівні відбувається автентифікація користувачів, через логін та пароль користувача, застосовуються біометричні засоби захисту, які забезпечують цілісність повідомлень. Також використовується хешування для генерування MAC, шифрування: RC5; 3DES; Rijndael, цифровий підпис: PKI, RSA, ECDSA, ECC [4].

Висновок. Проаналізовано аспекти захисту інформації у мережах рухомого зв'язку з урахуванням процедур перетворення інформації в цифровій системі зв'язку та процедур оброблення, зберігання відомостей інформаційною системою.

Список бібліографічних посилань

1. Конституція України : закон України від 28.06.1996 № 254к/96-ВР // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 (дата звернення: 10.11.2018).

2. FIPS PUB 140-2. Security Requirenments for Cryptographic Modules // U.S. Department of Commerce, NIST, 2001.

3. Stoneburgnen, G. CSPP-OSCOTS Security Protection Profile – Operating Systems. Draft Version 0.4 // U.S. Department of Commerce, NIST, 2005.

4. Ленков С. В., Перегудов Д. А., Хорошко В. А. Методы и средства защиты информации. Том 2. Информационная безопасность. Арий, 2008. 344 с.

Одержано 30.10.2018